

Information and Network Security



Lecture 1+2: introduction

Dr. Bhaa Alhmdan

المحتويات

المرجع



Cryptography and Network Security: Principles and Practice; By William Stallings.

طالما لديك شيء ذو قيمة سيعمل أحدهم على سرقته



أهمية أمن المعلومات



لماذا نظم امن المعلومات: ? What Information System Security

يمكن أن يتضح لنا الموضوع أكثر إذا نظرنا إليه في العالم الفيزياني:

- عند ما يريد شخص إرسال رسالة مهمة فإنه يتخذ كافة التدابير الأمنية اللازمة التي يعتقد أنها تضمن الحماية والوصول الامن لرسالته.
- وفي المؤسسات غير المؤتمتة مثلاً يتم حفظ الأوراق الهامة في خزائن لها أقفال غير قابلة للنسخ، ومحاولة تأمين عملية نقل آمنة لهذه الأوراق.
- أما في المؤسسات المؤتمتة مثل الشركات الكبيرة فلا يستخدم الورق نهائياً لذلك هم بحاجة لتأمين الاحتياجات الأمنية ولكن بشكل رقمي.

كما أنه عند إرسال رسالة يجب التأكد من مصداقية مصدر الرسالة وضمان عدم إطلاع أي شخص على الرسائل.

ولكن يا ترى العالم المؤتمت أكثر أماناً من العالم الفيزياني؟؟؟

نعني بمصطلح Information security حماية المعطيات ومعلومات النظام من أي وصول غير مصرّح له أو استخدام أو تعديل أو تدمير هذه المعلومات..

أهمية أمن المعلومات



يتكون النظام المعلوماتي من الممتلكات assets التالية :

- البيانات والمعلومات .
- العتاديات Hardware : الحاسب و توابعه من وحدات تخزين وأجهزة طرفية.
- البرمجيات Software : بكافة أنواعها سواء كانت أساسية أو تطبيقية .
- الشبكات و خدمات الاتصال

يضاف إلى ذلك :

- الأشخاص : مدير النظام والمستخدمون .

أهمية أمن المعلومات

- التهديد threat :
أي كائن أو شخص ممكن أن يشكل خطر مستمر على الممتلكات assets .

- الثغرة vulnerability :
ضعف محدد في النظام المعلوماتي الخاضع للرقابة أو الحماية ، مثل كون النظام المعلوماتي قابل للخرق أو يتضمن نظام حماية غير فعال أو محدث .

- الهجوم attack :
الفعل الذي يستغل الضعف في النظام الخاضع للحماية أو الرقابة .

تعريف الأمن :

نقصد بالأمن " في هذا السياق " حالة كون النظام المعلوماتي خال من أي مخاطر ، أي حماية كل مكونات النظام المعلوماتي المعرفة أعلاه من أي خطر. و هناك ثلاث مصطلحات تستخدم في هذا السياق و هي :

أهمية أمن المعلومات

What is the difference between a threat, a vulnerability, and a risk?



Threat:
Something that can damage or destroy an asset



Vulnerability:
A weakness or gap in your protection



Risk:
Where assets, threats, and vulnerabilities intersect



أهمية أمن المعلومات

- Security is "protection of assets (الأشياء القيمة) (resources) against threats."

- System Resource (Asset) - Data; a service provided by a system; a system capability; an item of system equipment.
- A Threat is a potential (ممكن) danger that might exploit a vulnerability. A threat can be:
  - Malicious (attackers, insider fraud, ...)
  - Accidental (natural disasters, human error (misuse), ...)

الأهداف الامنية

Security goals

We will first discuss three security goals: ***confidentiality***, ***integrity*** and **availability**



Security goals

الأهداف الامنية

The National Institute of Standards and Technology (NIST) Computer Security handbook defines the term Computer Security as:

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources"

Some people define additional major security objectives, while others lump those additional goals as special cases of these three.

الأهداف الامنية

The CIA Triad

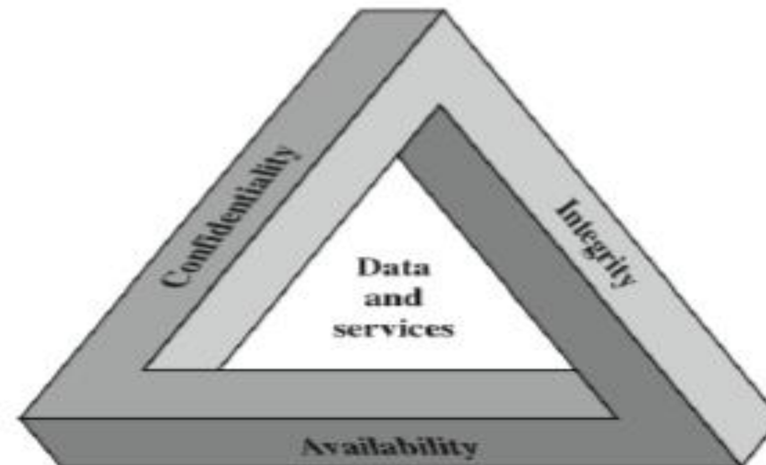


Figure 1.1 The Security Requirements Triad

الأهداف الامنية



What is CIA in information security??

يمكن تعريف امن المعلومات بطرق أخرى :

- تامين CIA وتعني :

- Confidentiality : عدم كشف المعلومات الا للأشخاص المخولين
- Integrity: السلامة , ان لا تتعدل المعلومات الا من قبل الأشخاص المخولين
- Availability : المعلومات متاحة لأصحاب الشأن وقت الحاجة

الأهداف الامنية

- مع ظهور شبكات الانترنيت واستخدام البريد الإلكتروني والمعاملات الإلكترونية ظهر هدفان جديدان هما:
- **المساءلة accountability:** توفير الإجراءات التي تمكننا من تحديد المسؤوليات عند القيام بعمل ما باستخدام النظام المعلوماتي. ومن ضمنها ما يسمى "عدم الإنكار non-repudiation" بحيث نوفر الأدوات التي تمنع مثلاً المرسل أو المستقبل لمعاملة ما من إنكار ذلك.
- **الأصالة Authenticity**: تعني التحقق من أن المستخدمين هم من يقولون أنهم هم , وأن كل مدخلات تصل إلى الوجهة تأتي من مصدر موثوق.

يضمن هذا المبدأ، إذا تم اتباعه، الرسالة الصحيحة والحقيقية المستلمة من مصدر موثوق من خلال إرسال صالح.

.

الأهداف الامنية

From: Cryptography and Network Security: Principles and Practice (7th Edition) by William Stallings

- Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.

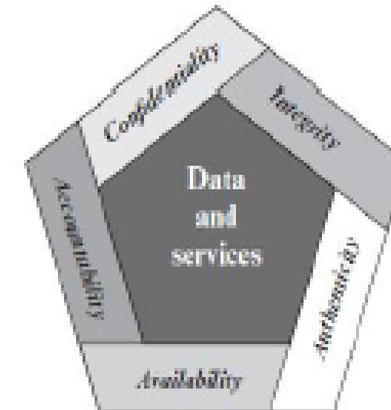


Figure 1.1 Essential Network and Computer Security Requirements

الأهداف الامنية

- *Authentication:*
is verification of identity (are you who you say you are).
Examples
include username/password and biometrics.

المصادقة هي التحقق من الهوية (هل أنت من تقول أنت) اما بالطرق التقليدية او بالعلامات الحيوية

- *Authenticity*
is verification of a message or document to ensure it wasn't forged تزويره or tampered with العبث به .
Examples
include digital signature and HMAC

موثوقية الرسالة وهي التحقق من الرسالة للتأكد من أنها غير مزورة ومن انه لم يتم العبث بها

What is Authorization
Authorization happens after a user's identity has been successfully authenticated. It is about offering full or partial access rights to resources like database, funds, and other critical information to get the job done.
In an organization, for example, after an employee is verified and confirmed via ID and password authentication, the next step would be defining what resources the employee would have access to

الأهداف الامنية



One of the most common method to authenticate identity is a password. If the user name matches the password credential بيانات الاعتماد it means the identity is valid, and the system grants access to the user.



Biometrics Authentication



الأهداف الامنية

- لتحقيق الاهداف الأمنية المطلوبة يتوجب تطبيق مجموعة من آليات الحماية وهي أليات مصممة من أجل منع وقوع هجمات أمنية أو كشفها أو التعافي منها بعد وقوعها ومن اهم هذه الآليات التشفير ، نظام كشف الدخلاء IDS وغيرها .. ولهذه الاليات نوعان أساسيان:

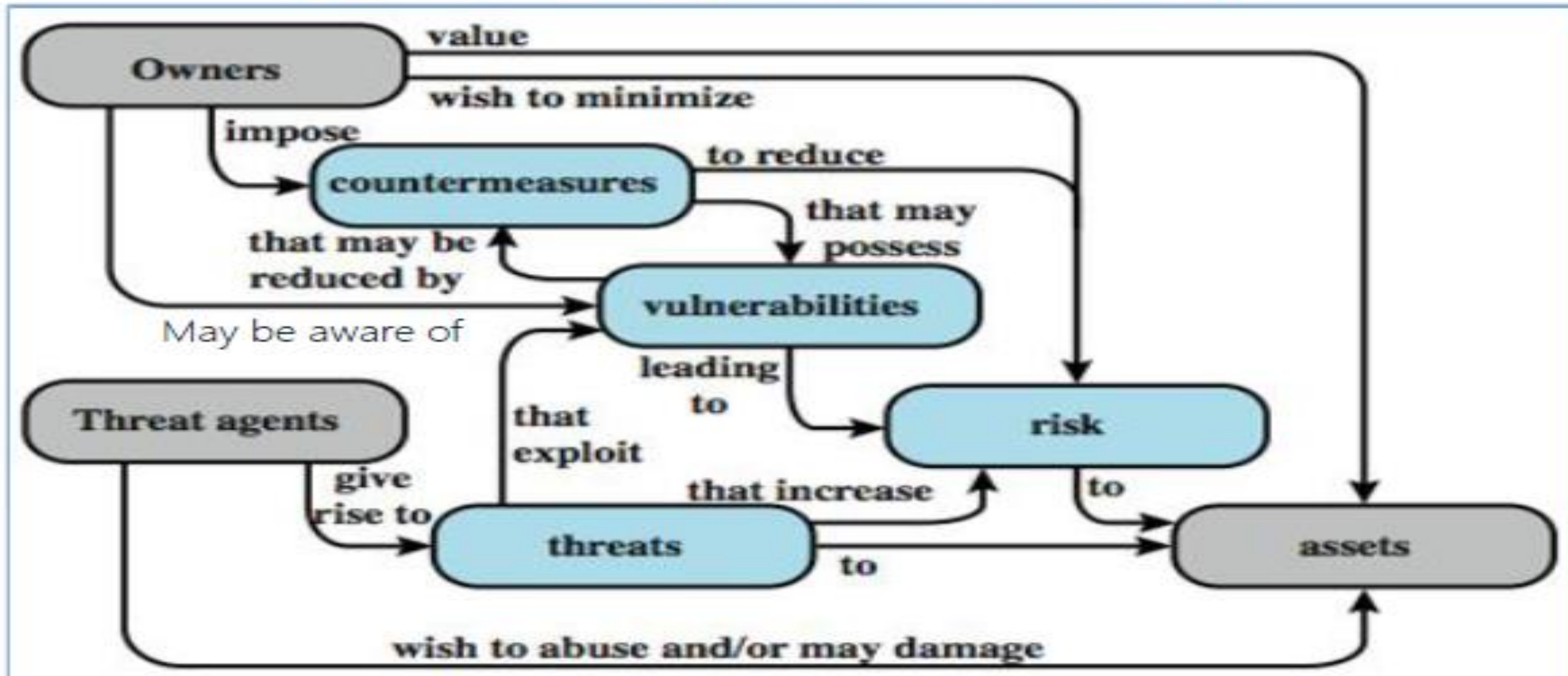
- Preventive: الإجراءات التي يتم اتخاذها من أجل **منع** تخريب الممتلكات (مثل : التشفير)
- Reactive:
  - Detection: الإجراءات التي يتم اتخاذها من أجل **تحديد** التخريب في الممتلكات .
  - Reaction: الإجراءات التي يتم اتخاذها **للتعافي** بعد الهجوم (مثل : النسخ الاحتياطي backup)

آليات حماية تُطبق لكشف الهجمات والتعامل معها (اي ان الهجوم سيقع والالية ستكشفه)

آليات حماية تُطبق لمنع وقوع الهجمات التي تستهدف المتطلبات الامنية

الأهداف الامنية

Security Concepts and Relationships



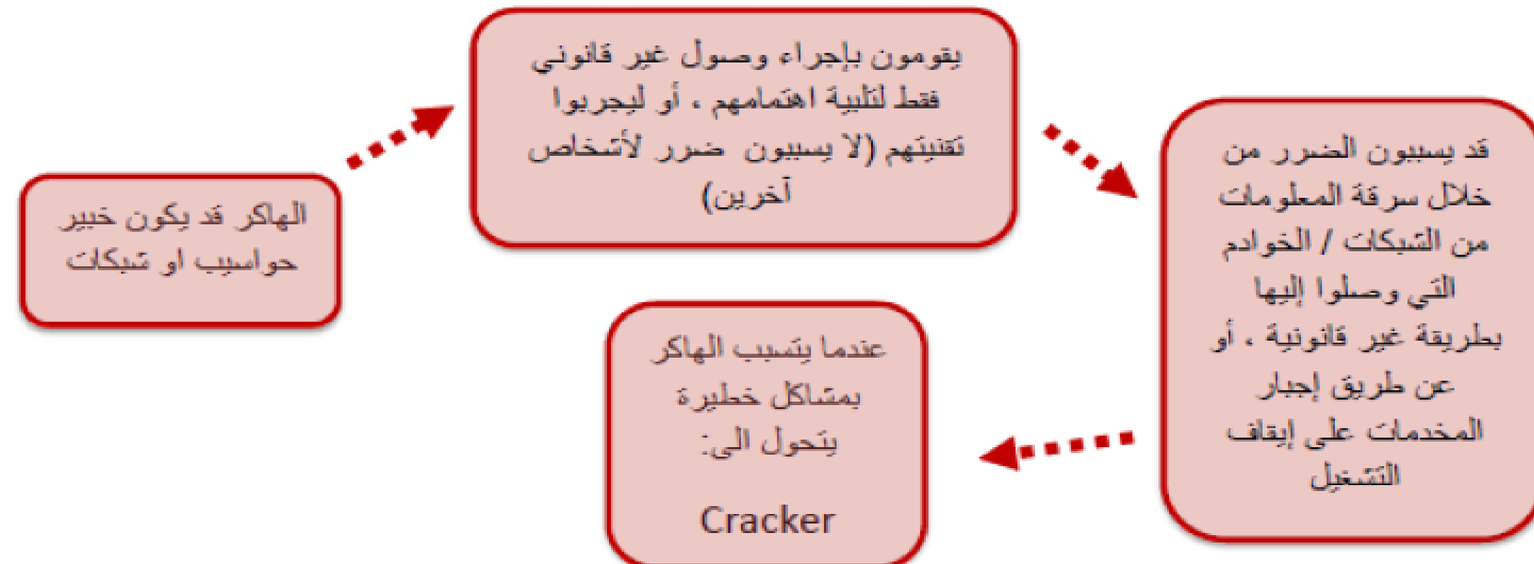
قرصنة المعلومات

Hacker – Cracker

- الهاكر - hacker: شخص لديه معرفة متقدمة بأنظمة التشغيل ولغات البرمجة قد يكتشف ثغرات داخل الأنظمة وأسباب هذه الثغرات قد يشارك ما اكتشفه ولكن لا يتلف البيانات مطلقا (نواياهم جيدة)
- cracker : (قراصنة الحواسيب)

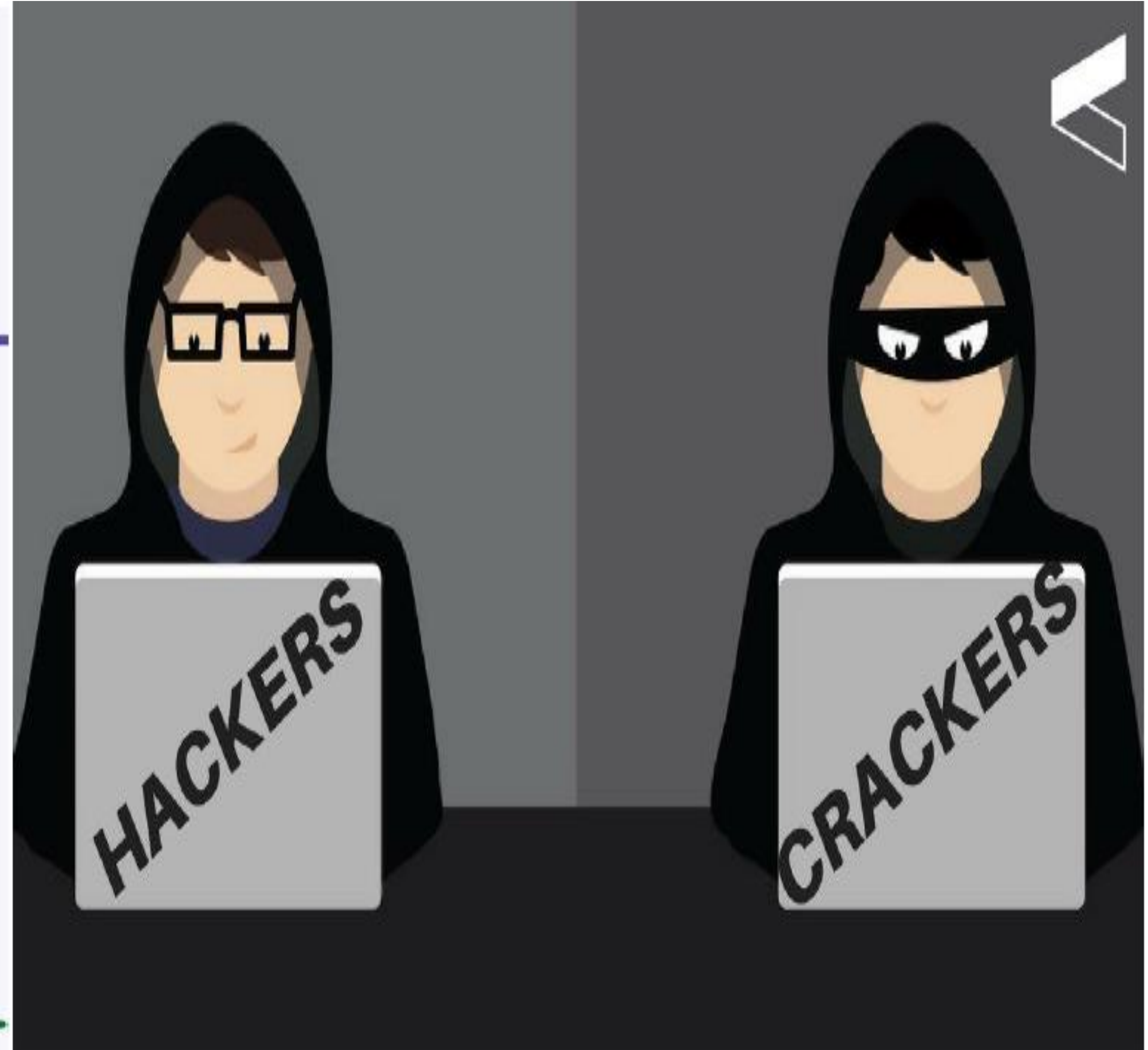
الشخص الذي يقتحم أو ينتهك سلامة نظام الأجهزة البعيدة بقصد خبيث ،

مثال : الحصول على وصول غير مصرح به , تدمير البيانات الحيوية ، وتنكر خدمات المستخدمين الشرعيين.



الأهداف الامنية

HACKER	CRACKER
	
• NEVER DAMAGE THE DATA.	• DELETE OR DAMAGE THE DATA.
• THE ETHICAL PROFESSIONALS.	• UNETHICAL PERSON ,DO ILLEGAL TASKS.
• HACKERS HAVE LEGAL CERTIFICATES.	• MOTIVE IS TO STAY ANONYMOUS.
• GOOD PEOPLE, HACK FOR KNOWLEDGE PURPOSES.	• EVIL PERSON WHO BREAKS INTO A SYSTEM FOR BENEFITS.



الأهداف الامنية

القرصنة الأخلاقية هي عملية اكتشاف الثغرات الأمنية في تطبيق أو نظام أو في البنية التحتية لمؤسسة ما والتي يمكن للمهاجم استخدامها لاستغلال الاشخاص أو المؤسسة.
تستخدم هذه العملية لمنع الهجمات الإلكترونية والانتهاكات الأمنية من خلال الاختراق القانوني للأنظمة والبحث عن نقاط الضعف

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization.
They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points.



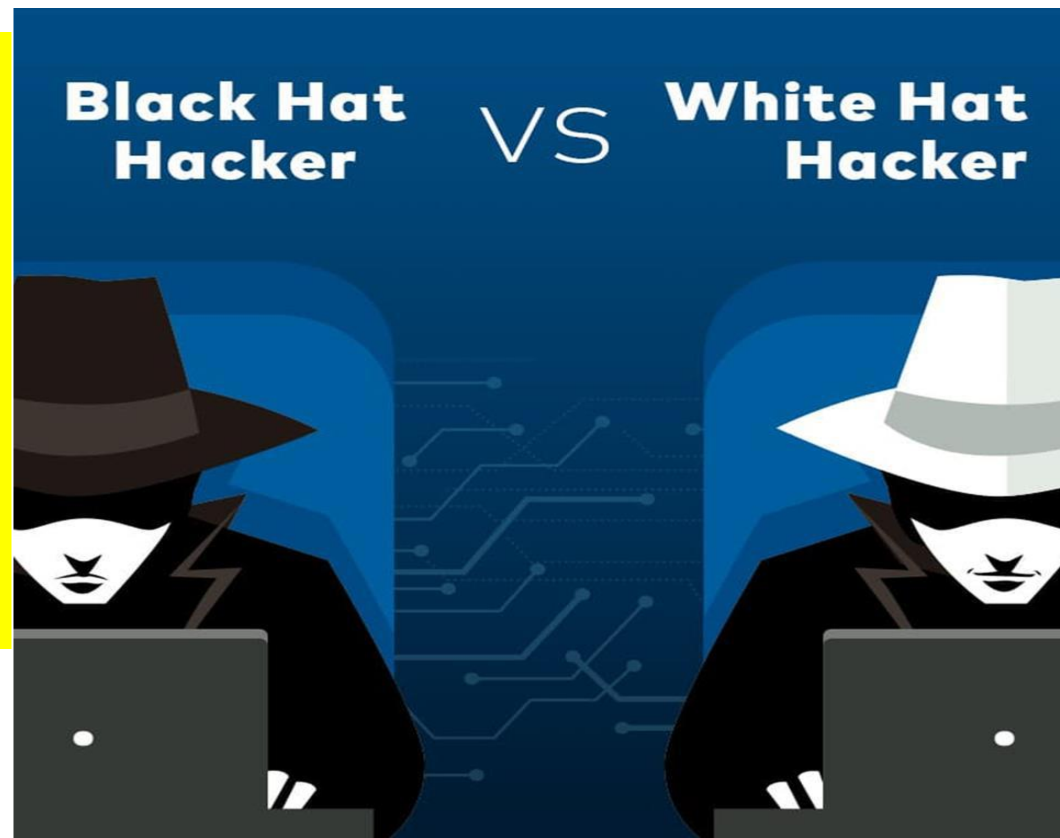


الأهداف الامنية

Ethical hackers are often referred to as 'white hats', while malicious hackers are 'black hats'.

Hacking is the act of gaining unauthorized access to data in a system or computer.
A Hacker is a person who exploits vulnerabilities in a computer system or network, plant a virus or steal information.

But not all hackers have bad intentions



The hackers use their knowledge to help security systems, and the crackers use their knowledge to break the laws and disrupt security. ... The Hackers being the good guys, are called white hats, while **black hats usually refer to the crackers which violate computer security for personal gains**

الـهجمات الأمنية الشائعة

التهديدات هي :

- Interruption, delay, denial of receipt or denial of service
- Interception or snooping
- Modification or alteration
- Masquerade or spoofing
- Repudiation
- Traffic analysis
- Replay attack

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an **attack** against confidentiality.

A masquerade attack is an attack that uses a **fake identity**, such as a network identity, **to gain unauthorized access to personal computer information** through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

Repudiation Attack – A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction

الـهجمات الأمنية الشائعة

1- Interruption, delay, denial of receipt or denial of service

Interruption وتعني المقاطعة , delay التأخير , denial of service حجب خدمة (رفض خدمة).

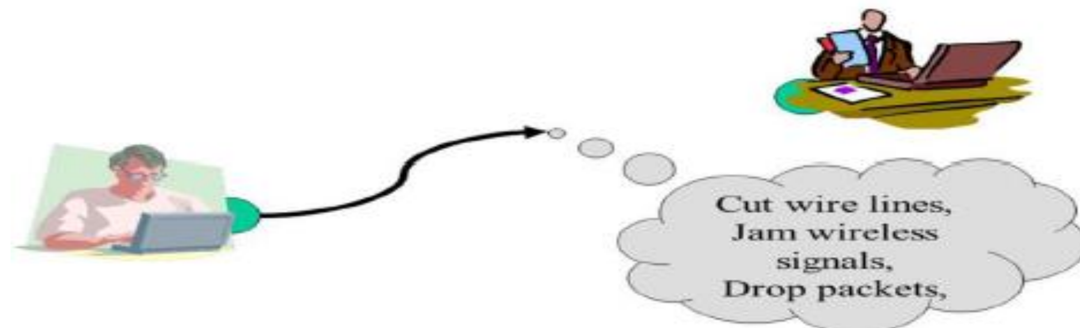
المقاطعة تستهدف الاتاحة .

والهجمات السابقة تؤدي الى جعل النظام او المعلومات غير متاحة وقت الحاجة .

كيف يمكننا مواجهة مثل هذا النوع من الهجمات ؟

بالإمكان القيام بعمليات back up وبدلا من ان يكون لدي server واحد يكون لدي 2 ,وبدل وجود بطاقة بطاقتين وهكذا....

Attack: Interruption

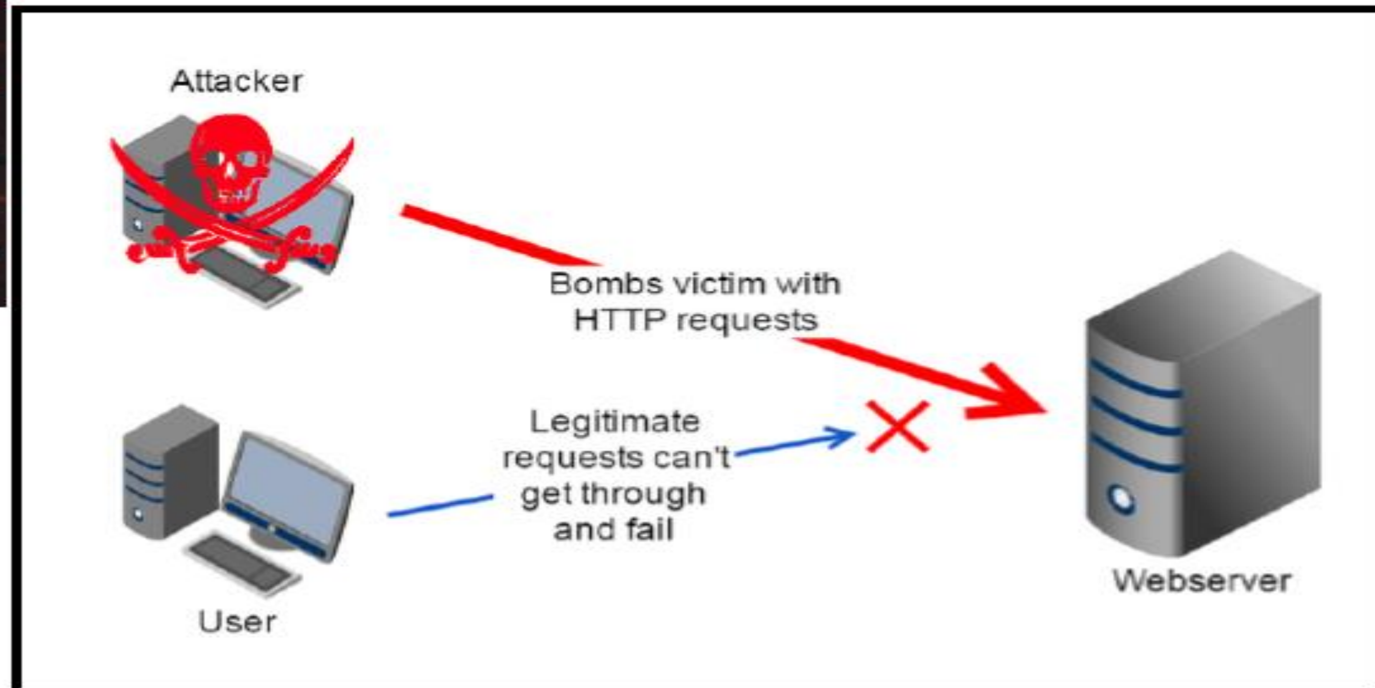


الـهجمات الأمنية الشائعة

1- Interruption, delay, denial of receipt or denial of service

A Denial-of-Service (DoS) attack is an **attack meant to shut down a machine or network**, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash



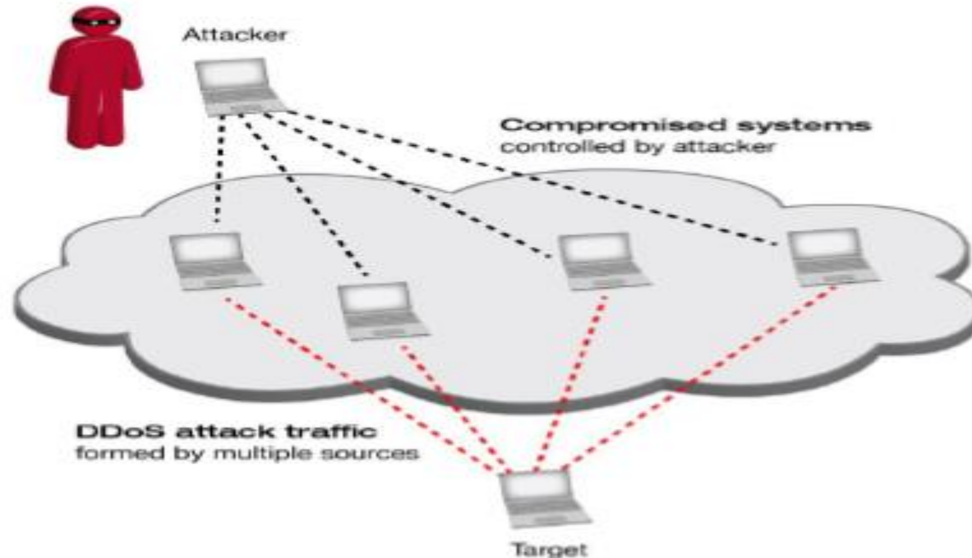


الـهجمات الأمنية الشائعة

1- Interruption, delay, denial of receipt or denial of service

يمكن القيام بـ DDOS (وهي distributed denial of service) حيث يقوم بالهجمة وقتها اكثر من شخص معا .

DDoS : It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.





الهجمات الأمنية الشائعة

2- Interception or snooping التنصت also known as a **sniffing** or **Eavesdropping attack**

- الاعتراض : فرضا تم ارسال رسالة من حساب مستخدم الى webserver فتم اعتراض الرسالة والحصول على password مثلا , فهو لا يعني منع الرسالة من الوصول لكن يقوم بأخذ نسخة عنها .
- Interceptor : هو الشخص الذي يأخذ الرسالة .
- Snooper : هو الذي يفتش على مستوى البيانات التي تمر عبر الشبكة او في الحواسيب وغيرها .

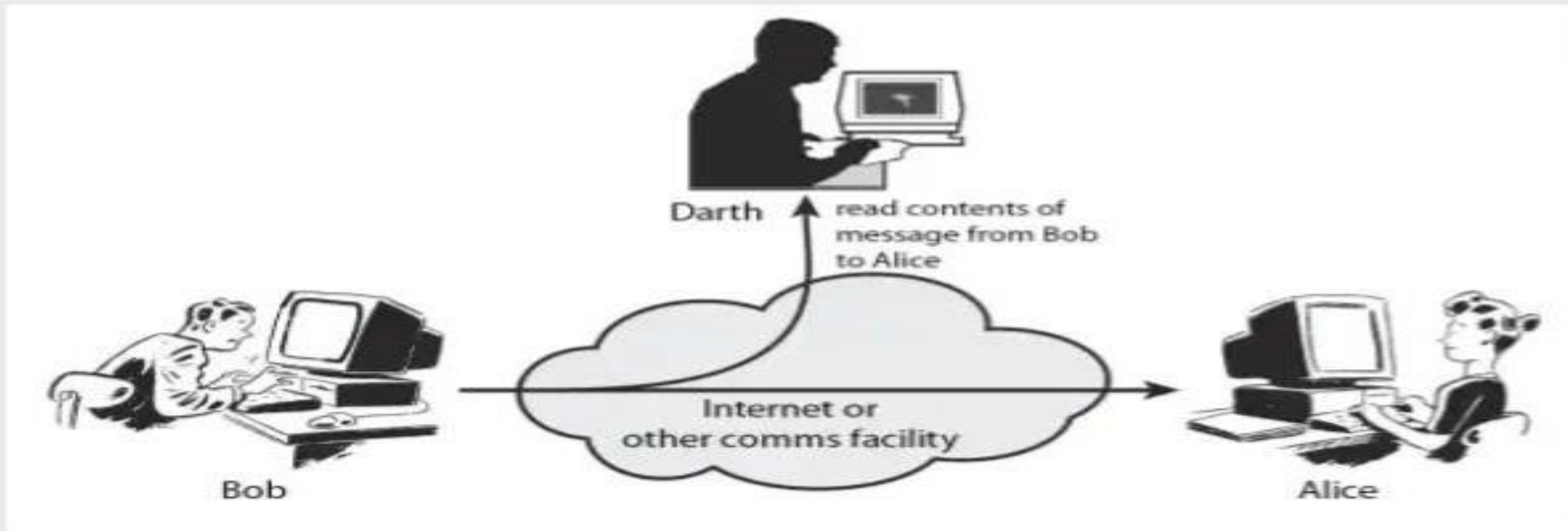
اعتراض البيانات يستهدف السرية

من اجل حل المشكلة يجب القيام بإجراءات الحماية عند النقل والادخال والتخزين فعند تحليل النظام نقول اننا يجب ان نؤمن سرية البيانات الشخصية وعند التصميم نقترح وضع كلمة مرور و access control ولكن وسيلة وضع كلمة المرور يجب أيضا ان تكون امنة حتى يتم تامين السرية .



الـهجمات الأمنية الشائعة

2- Interception or snooping التنصت also known as a **sniffing** or **Eavesdropping attack**



الهجمات الأمنية الشائعة

2- Interception or snooping التنصت also known as a **sniffing** or **Eavesdropping attack**

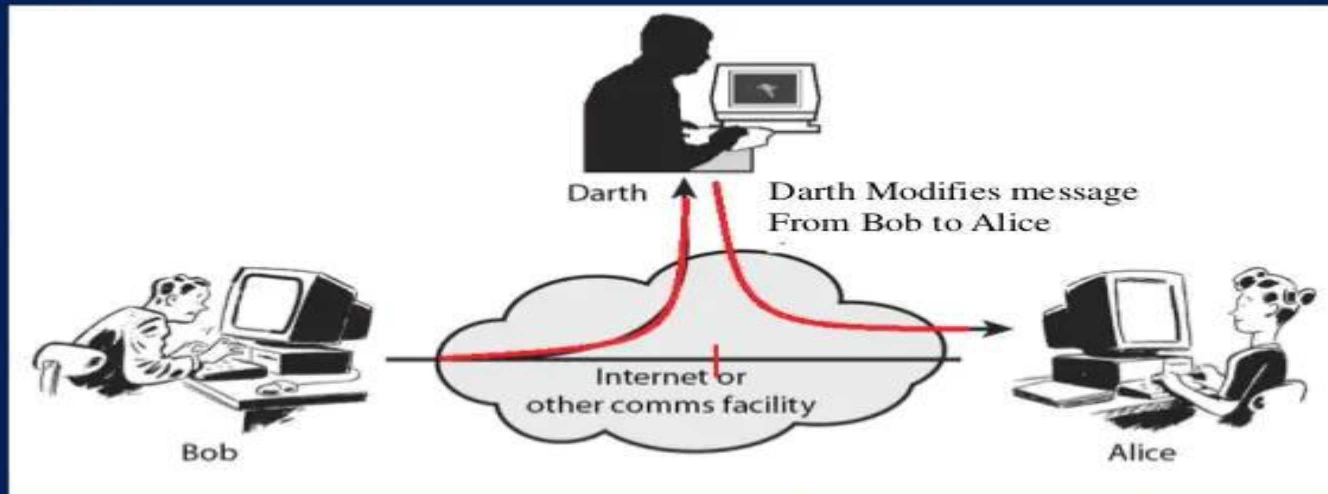


الهجمات الأمنية الشائعة

3- Modification or alteration

التعديل يستهدف السلامة

الأشخاص غير المخولين يقومون بتعديل البيانات خلال نقلها او تخزينها لاهداف شخصية .



الهجمات الأمنية الشائعة

4- Masquerade or spoofing

- Masquerade : انتحال الشخصية .
- Spoofing : وتعني هنا ارسال رسالة او طرد شبكي بغير عنوان المرسل الحقيقي

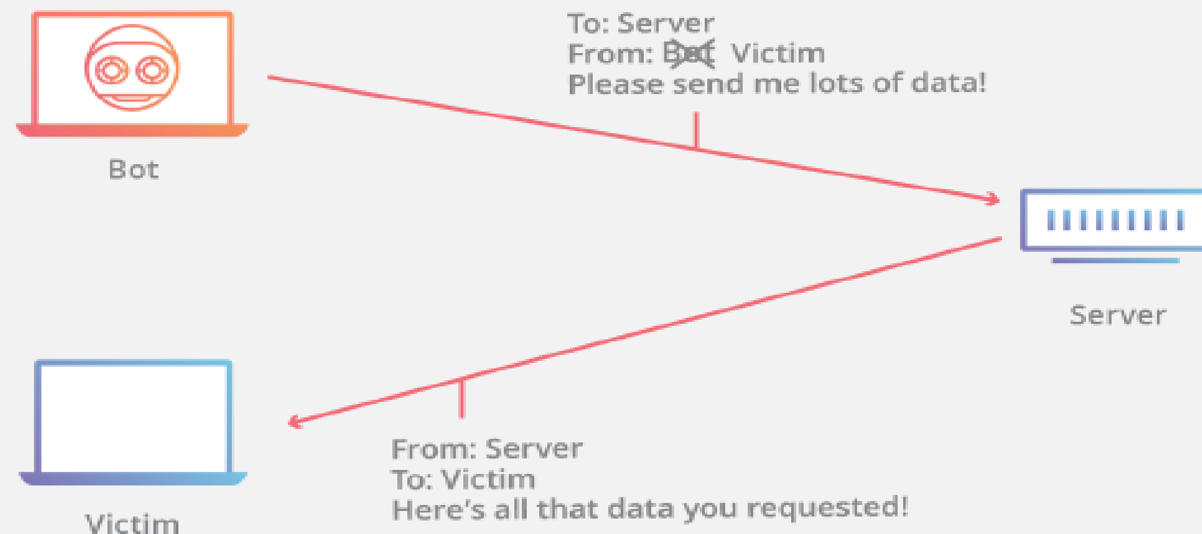
التزييف

تستهدف الوثوقية او الاستيقان

من اجل حل المشكلة يجب التأكد من هوية الشخص عبر authentication (authenticity).

ما يقوم masquerade بفعله هو جعل المعلومات تبدو وكأنها قادمة من كيان موثوق .

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address <u>in order to either hide the identity of the sender</u>



الهجمات الأمنية الشائعة

How Masquerade Attack Works



Jack
(Daniel Friend)





Hacker Darth



Daniel

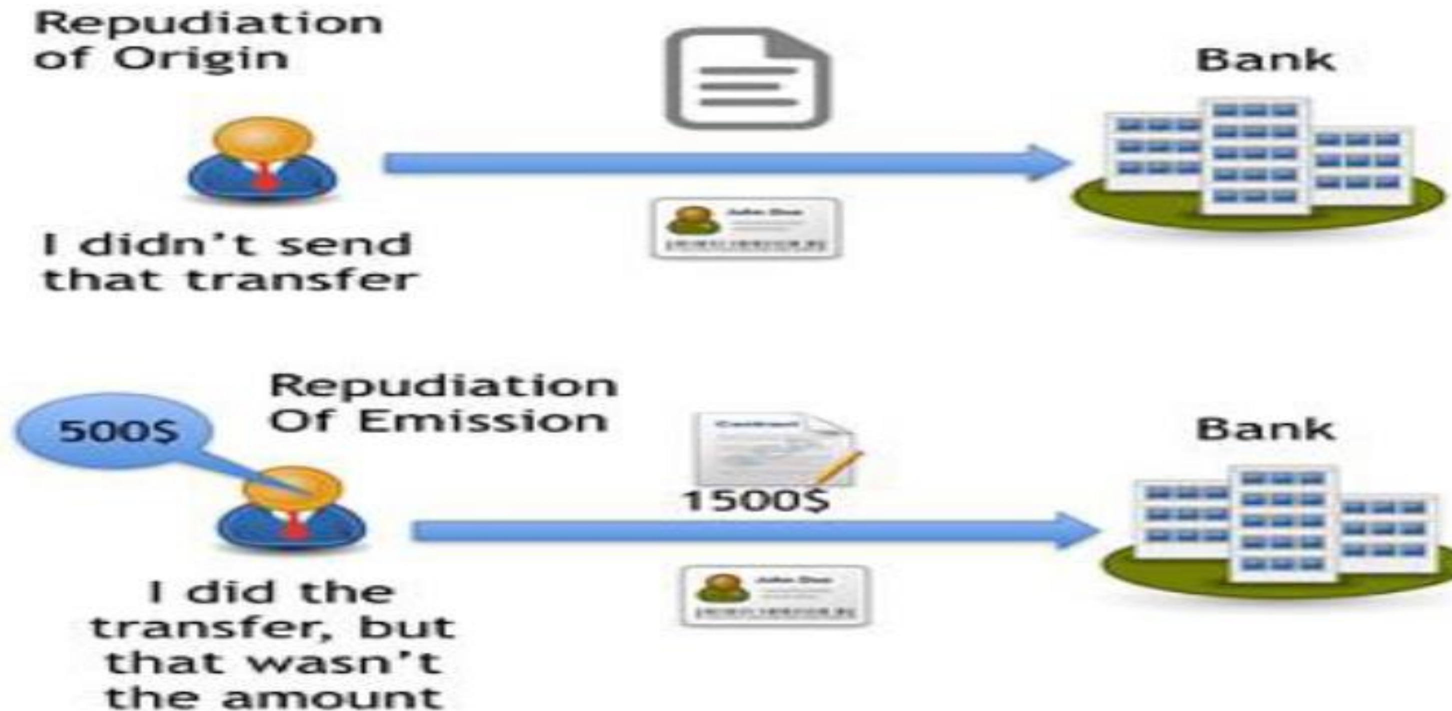
Message From Hacker Darth that appears to be from Jack

الهجمات الأمنية الشائعة

5- Repudiation

وتعني انكار المشاركة في الاتصال . تهديد لمتطلب عدم الانكار

يمكن ل sender ان يقوم بالإنكار ويمكن ل receiver ان يقوم بالإنكار وتستعمل في التطبيقات والمعاملات المالية .

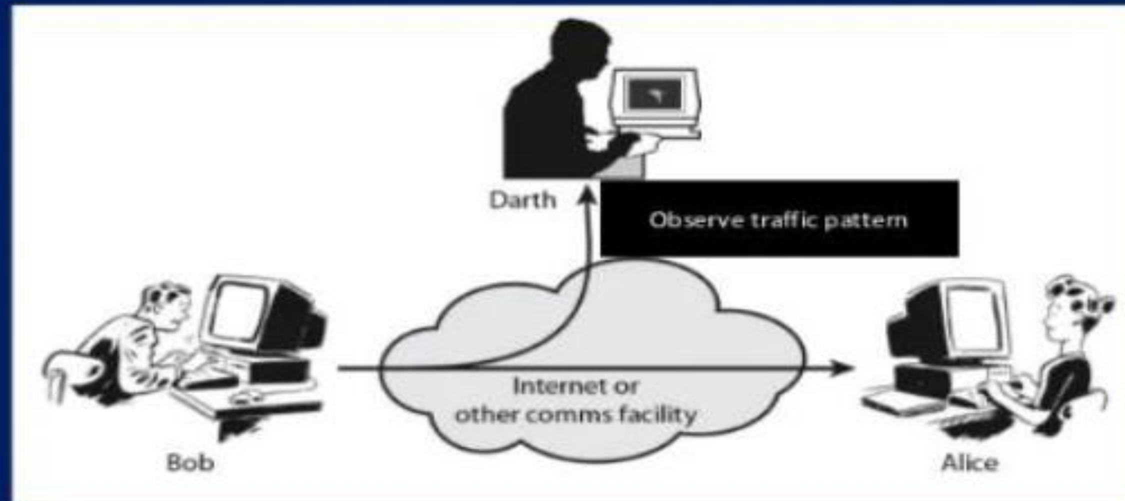


الـهجمات الأمنية الشائعة

6- Traffic analysis

تحليل المرور الشبكي .

تحليل المرور الشبكي هو مرحلة من مراحل الهجوم .



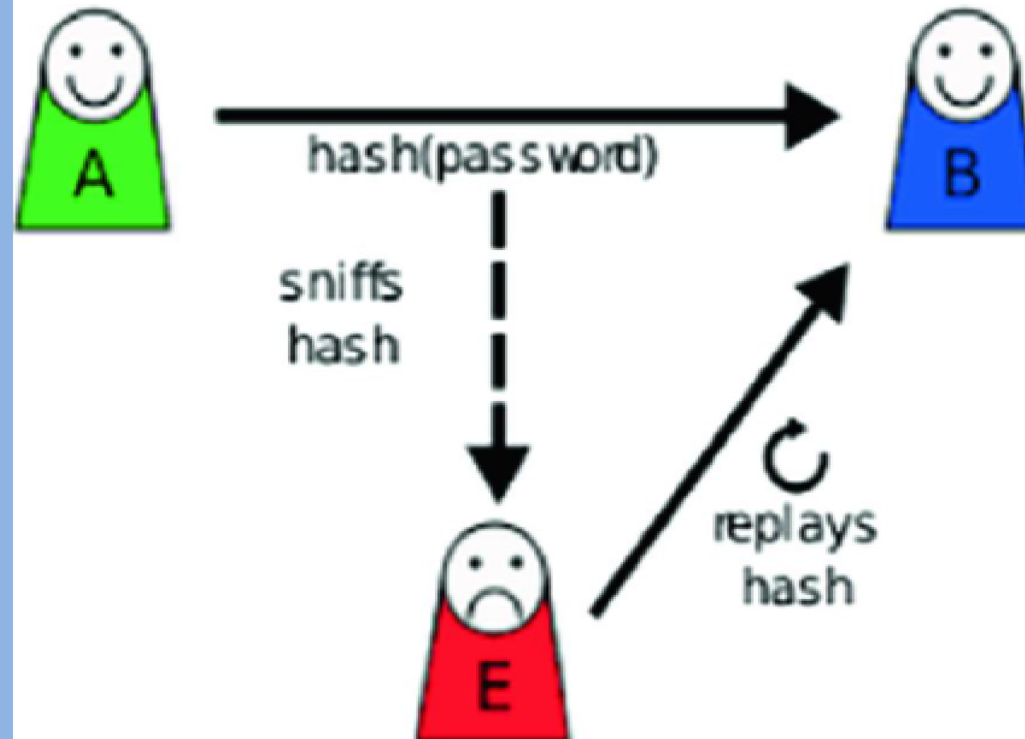
الهجمات الأمنية الشائعة

7- Replay attack

إعادة الارسال .

One **example** of a **replay attack** is to **replay** the message sent to a network by an attacker, which was earlier sent by an authorized user

In a replay attack, it doesn't matter if the attacker who intercepted the original message can read or decipher the key. All he or she has to do is capture and resend.
To counter this possibility, both sender and receiver should establish a completely random session key, which is a type of code that is only valid for one transaction and can't be used again.
Another preventative measure for this type of attack is using timestamps on all messages. This prevents hackers from resending messages sent longer ago than a certain length of time



مصطلحات هامة

Backdoors – Backdoor is a type of cyber threat in which the attacker uses a back door to install a keylogging software, thereby allowing an illegal access to your system.

What Is a Keylogger?

Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders. Keylogger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

مصطلحات هامة



Social Engineering – An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.

Malware – Malware refers to malicious software that are being designed to damage or perform unwanted actions into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer's hard drive. They can either delete some files or a directory or simply gather data without the actual knowledge of the user.

مصطلحات هامة

Adware – Adware is a software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.

Bots – Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be malicious, but they are usually found to initiate a DoS attack.

Ransomware – Ransomware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.

مصطلحات هامة

- Vulnerability - Flaw (خطأ)or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.



- Attack - A deliberate (متعمدة) attempt to evade security services and violate security policy of a system.
- Adversary (threat agent) (الخصم) - An entity that attacks, or is a threat to, a system.

مصطلحات هامة

- Risk - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

(المخاطرة : توقع الخسارة ويعبر عنه من خلال احتمال أن تهديد معين سيستغل ثغرة أمنية معينة ليؤدي الى نتيجة ضارة معينة.)

- Security Policy - A set of rules and practices that specify how a system or organization provides security services to protect sensitive and critical system resources.
  - Standards like: ISO/IEC 27002 and ISO 27001.

مصطلحات هامة

- Countermeasure (مضاد)- An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by **eliminating** or **preventing** it, by **minimizing** the harm it can cause, or by **discovering** and **reporting** it so that corrective action can be taken.

(المضاد : فعل، أداة (جهاز) ، إجراء ، أو تقنية تقلل من التهديد ، الثغرة ، أو الهجوم من خلال القضاء عليه أو منعه ، من خلال تقليل الأذى الذي يمكن أن يحدثه إلى أقل مايمكن أو من خلال اكتشافه و الإبلاغ عنه حتى يتم اتخاذ اجراءات تصحيحية.)

تصنيف الهجمات الأمنية

 **الهجمات غير الفعالة Passive Attacks:**

يكون هدف المهاجم في هذا النوع من الهجمات تجميع المعلومات، فهو لا يقوم بتعديل المعلومات أو بالتسبب بأي أذى للنظام الحاسوبي. يمكن لعملية تجميع المعلومات أن تسبب أذى للمرسل أو المستقبل لكنها لا تؤثر على النظام الحاسوبي الذي يتابع عمله بشكل طبيعي. تعتبر الهجومات المهددة للسرية هجمات غير فعالة، وهي هجمات من الصعب جدًا التقاطها حتى يكتشف المرسل أو المستقبل تسرب معلومات سرية تخصه. يمكن منع هذا النوع من الهجومات من خلال تشفير المعطيات.

تصنيف الهجمات الأمنية

- الهجمات الفعالة Active Attacks:

يتسبب هذا النوع من الهجومات بتغيير المعطيات أو بأذى للنظام الحاسوبي. تعتبر الهجومات المهددة للتكامل والإتاحية من هذا النوع، ومن السهل التقاطها أكثر من منعها لأن المهاجم يقوم بتنفيذها بعدة أساليب وطرق.

تصنيف الهجمات الأمنية



الهجمات السلبية Passive Attacks : الهدف منها هو الحصول على المعلومات المنقولة لتميز محتوى الرسالة وتحليل سيالة المعلومات الجارية.

1- **محتوى الرسالة:** قد يحتوي على معلومات سرية وحساسة لذلك يجب منع الهجمات على المعلومات.

2- **تحليل سيالة المعلومات :** يمكن استخدام التعمية في عملية التمويه لمنع المهاجم من الاطلاع على مضمون الرسائل وبالتالي كامل سيالة المعلومات.

يعتبر من أنواع الهجوم صعب الاكتشاف وبالتالي يجب التركيز لمنعه وليس لاكتشافه.

تصنيف الهجمات الأمنية



الهجمات الفعالة **Active Attacks** : تعتمد على إجراء تعديلات على سيالة المعلومات أو إنشاء سيالة كاذبة ويقسم إلى:

1- **هجوم التخفي Masquerade**: تقديم شخص نفسه على أنه شخص آخر بعد تحديد هوية الأول.

2- **هجوم إعادة البث Replay Attacks**: التقاط معطيات ما ثم إعادة إرسالها من أجل التشكيك.

3- **هجوم التعديل Modification of Messages**: تغيير جزء من رسالة ما أو تغيير ترتيبها ومعناها.

4- **هجوم حجب الخدمة Denial of Service**: منع مرور كل الرسائل الموجهة لجهة ما أو تعطيل الشبكة الكلية عن طريق تحميل زائد للرسائل وإرسالها.

الأدوات الأمنية

- **التشفير Encipherment**: تفيد هذه الأداة في إخفاء المعطيات للحفاظ على سريتها. يمكنأيضًا استخدامها كتتمة وتكملة للأدوات الأخرى اللازمة لبناء خدمة أمنية. يتوفر لدينا حالياً تقنيتان للتشفير ، هما:

التعمية **Cryptography** والتورية **Steganography**

- **التحكم بالوصول Access Control** : يمكن اللجوء إلى هذه الأداة لتحديد سماحيات وصول المستخدم إلى المعطيات والمصادر المملوكة من قبل النظام، مثل: السماحيات الممنوحة وفقاً لكلمات السر **Passwords** أو الرموز السرية **PINs**

الأدوات الأمنية

- تكامل المعطيات Data Integrity: تفيد هذه الأداة في إضافة بعض المعلومات الإضافية(مجاميع قصيرة للتحققShort checkvalues)وفقًا لإجراء معين إلى المعطيات نفسها قبل إرسالها. يقوم المستقبل باستقبال المعطيات مع مجاميع التحقق، ثم يحاول حساب هذه المجاميع بنفسه على المعطيات الحقيقية للتحقق من صحة المجاميع. إذا تطابقت المجاميع فهذا يعني أنه جرى المحافظة على تكامل المعطيات.

- التوقيع الإلكتروني Digital Signature : تفيد هذه الأداة في توفير إمكانية توقيع المرسل للمعطيات المرسلة من قبله الكترونياً بحيث يمكن للمستقبل أن يتحقق من هذا التوقيع عنداستلام المعطيات للتأكد من هوية المرسل يتم ذلك باستخدام المفتاح الخاصKey Private بالمرسل لتوقيع المعطيات قبل إرسالها، ثم يستخدم المستقبل المفتاح العام Public Key. للمرسل والمعروف من قبل الجميع للتحقق من صحة التوقيع على نفس المعطيات المستقبلة من قبله

الأدوات الأمنية

- تبادل التعارف Authentication Exchange: تعني هذه الأداة أن طرفي الاتصال يتبادلان بعض الرسائل ليتحقق كلٌّ منهما من هوية الآخر. يمكن مثلاً أن: يثبت أحد الطرفين أنه يعلم سراً لا يفترض بأحد آخر أن يعرفه.
- حشو المعطياتTraffic Padding: ويفيد ذلك في إدراج كمية من المعطيات غير المفيدة ضمن المعطيات الحقيقية بحيث تصبح هذه المعطيات بمجملها مضللة لهجمات تحليل حركة المعطيات.
- التحكم بالتوجيه Routing Control ويعني ذلك اختيار طرق توجيه مختلفة بين المرسل و المستقبل و التبديل بينها من وقت إلى آخر لتضليل المتصنت على أحد هذه الطرق المتاحة.
- المرور بطرف ثالثNotarization : ويعني ذلك اختيار طرف ثالث موثوق به للتحكم بالاتصال بين طرفين آخرين. يمكن اللجوء إلى هذه الأداة لمنع الإنكار. يمكن مثلاً أن: يلجأ المستقبل باختيار طرف ثالث موثوق به لتخزين طلبات المرسل بهدف منعهمن الإنكار لاحقًا بأنه أرسل هذه الطلبات.

الأدوات الأمنية

- الأخفاء Steganography :

✓ الاخفاء أو الكتابة المخفية هو فن وعلم قديم .

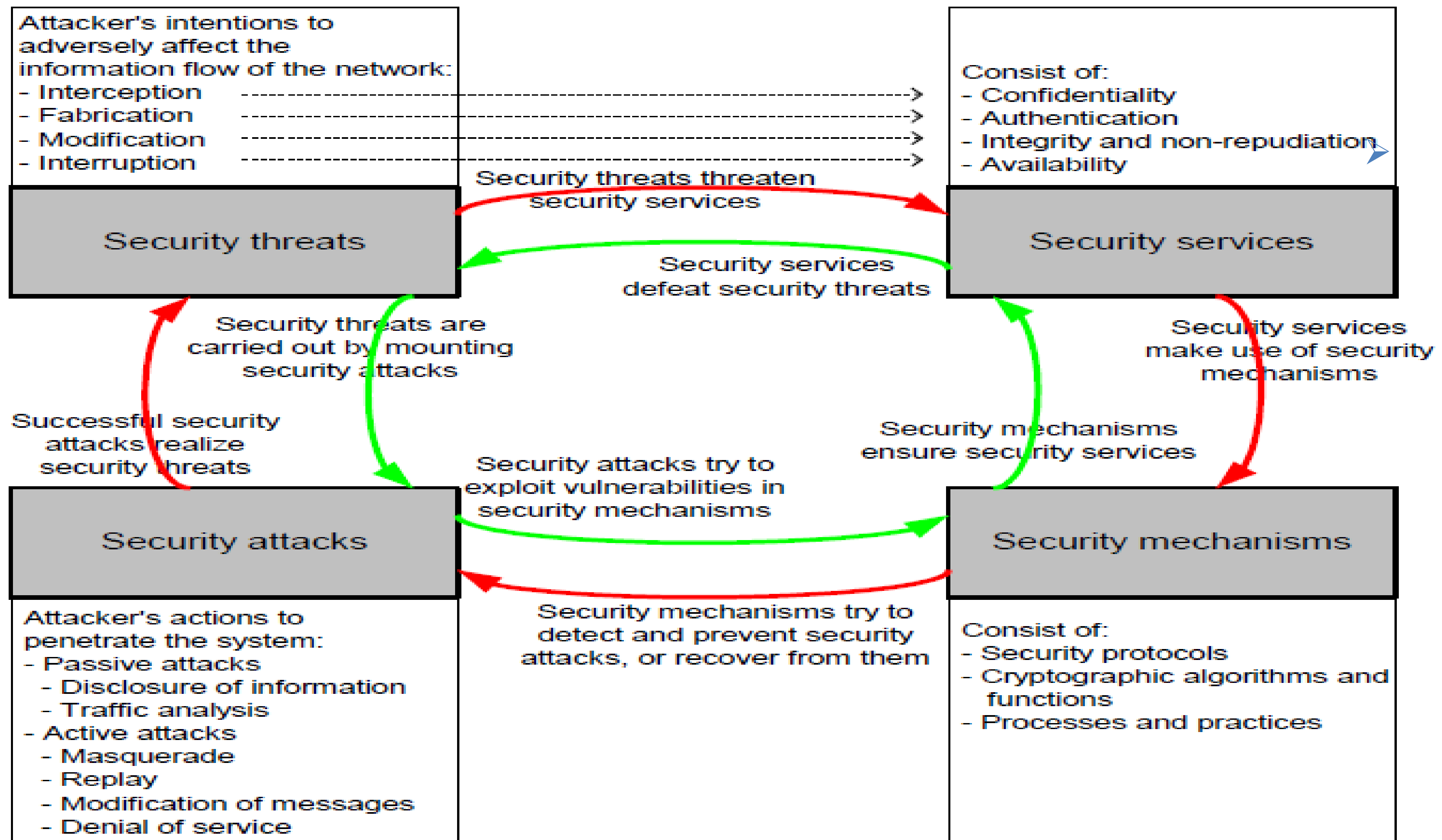
✓يعبر عن الرسالة المخفية بالمحمول، وعن الكائن الحاوي لها بالحامل (صورة ، أو رسالة أخرى ، أو مقطع فديو).

✓تم تطوير هذا العلم ليعمل وفق خوارزميات محددة ومن أهمها خوارزمية البت الأقل أهمية Lest Significant Bit (LSB).

✓يجب مراعاة طول الرسالة السرية وعمليات الحشو عند اللزوم .

✓يمكن استخدام هذا التقنية بشكل مستقل أو بالتعاون مع تقنيات التشفير .

Summary


Attacker's intentions to adversely affect the information flow of the network:
- Interception
- Fabrication
- Modification
- Interruption
Consist of:
- Confidentiality
- Authentication
- Integrity and non-repudiation
- Availability
Security threats threaten security services
Security threats
Security services
Security services defeat security threats
Security threats are carried out by mounting security attacks
Security services make use of security mechanisms
Successful security attacks realize security threats
Security mechanisms ensure security services
Security attacks try to exploit vulnerabilities in security mechanisms
Security attacks
Security mechanisms
Security mechanisms try to detect and prevent security attacks, or recover from them
Attacker's actions to penetrate the system:
- Passive attacks
- Disclosure of information
- Traffic analysis
- Active attacks
- Masquerade
- Replay
- Modification of messages
- Denial of service
Consist of:
- Security protocols
- Cryptographic algorithms and functions
- Processes and practices

مستويات حماية المعلومات

- المستخدم
- مستوى التطبيق
- مستوى النظام
- الحاسب
- الشبكة المحلية LAN
- الربط مع الشبكة الخارجية LAN to WAN
- الشبكة الخارجية WAN
- الوصول عن بعد
- المخدمات والبنية التحتية

مستويات حماية المعلومات

❑ المستخدم:

- نقطة الضعف في أي نظام وليس فقط نظام المعلومات، في هذا المستوى يجب مراعاة مستوى الموظف ويجب وبشكل مستمر إخضاعهم لدورات تدريبية مختلفة بهدف زيادة وعيهم تجاه المخاطر الأمنية المختلفة ابتداءً من عدم قدرتهم على عدم تمييز بريد التصيد من البريد النظامي وتطبيق أنظمة تحديد صلاحيات تمنع الموظفين من الوصول للملفات والتطبيقات التي لا يحتاج إليها لأداء مهامه.

- كما يجب الانتباه إلى الموظف "القرفان" وهو الموظف الذي يكره عمله وقد يكون على استعداد لأذية الشركة ولذلك يجب تتبع ومراقبة الموظفين ومستوى راحتهم في العمل وملاحظة الحالات التي يمكن أن تؤدي إلى أذية الشركة، علماً أن هذه ليس من صلاحيات قسم الـ IT وإنما قسم إدارة الموارد البشرية ومدراء الأقسام.

مستويات حماية المعلومات

❑ مستوى التطبيق:

- يعبر هذا المستوى عن مقدار الأمان الموجود ضمن تطبيق الشركة الذي يتم التعامل معه أو التطبيقات الإضافية التي يتم استخدامها مثل المتصفح أو برنامج MS Word
  - ✓ 99% من البرامج الحالية تتضمن اتصال مع الإنترنت وفي حال تواجدت ثغرة ضمن هذه البرامج يمكن الدخول وأذية الشركة من خلالها.

مستويات حماية المعلومات

❑ مستوى النظام:

- تشير إلى المستوى الأمني الموجود ضمن نظام التشغيل نفسه
- يعتبر نظام التشغيل مجموعة كبيرة من البرامج المختلفة التي تعمل مع بعضها البعض لإدارة موارد النظام، يمكن في كثير من الأحيان وجود ثغرات أمنية ضمن هذه البرامج يمكن استخدامها للدخول إلى الشركة
- مثل الثغرة ضمن بروتوكول SMB المستخدم لمشاركة الملفات ضمن Windows والتي تم استثمارها من قبل برمجية WannaCry لتضمن لنفسها الانتشار ضمن الشبكة المحلية.
- كما لا ننسى التعاريف Drivers التي تضمن تواصل النظام مع العتاد وفي بعض الأحيان يمكن أن توفر ميزات برمجية إضافية للنظام مثل نظام Falcon Sensor
- تسبب تحديث سيء لنظام الحماية Falcon Sensor بخروج ملايين من أجهزة Windows من الخدمة في 7 آب 2024 للعلم (Falcon Sensor) عبارة عن نظام حماية من البرمجيات الضارة.

مستويات حماية المعلومات

❑ الحاسب:

- تمثل محطة العمل أي حاسب مكتبي، محمول أو جهاز متنقل متصل بالشبكة سلكياً أو لا سلكياً، ومن النقاط التي يجب مراعاتها هي استخدام كلمات المرور لضمان الوصول للحواسيب والتجهيزات وتفعيل القفل التلقائي للتجهيزات في حال عدم استخدامها لمدة زمنية محددة، بالإضافة لضبط الوصول إلى التطبيقات حسب حاجة المستخدمين وإضافة كلمة مرور للتجهيزات الحساسة.
- كما يجب أن لا ننسى أنه في بعض الأحيان توجد ثغرات أمنية ضمن العتاد نفسه وما ثغرتا Specter وMeltdown ضمن معالجات Intel وAMD إلا مثال على ذلك

مستويات حماية المعلومات

❑ الشبكة المحلية LAN:

- عليًنا وبشكل دوري التأكد من سلامة التمديدات السلكية وأن خزن الشبكة مغلقة ولا يمكن الوصول إليها بسهولة ووضع المخدمات ضمن غرف لا يمكن الوصول إليها إلا من مقبل موظفين مختصين، كما يجب استخدام تقنيات تسجيل دخول إلى الشبكة اللاسلكية باعتماد اسم مستخدم وكلمة مرور (Radius) لأن ذلك يسمح بتتبع المشاكل التي تحصل في الشبكة، كما يجب مراقبة نشاط الشبكة بشكل مستمر للتأكد من عدم وجود برمجيات خبيثة فيها.

❑ الشبكة الخارجية WAN:

- عادةً تعبر الشبكة الخارجية عن شبكة الأنترنت، وبالتالي تتميز هذه الشبكة بمستوى الأمان المنخفض فيها، إذ معظم البيانات يتم إرسالها بشكل نصي بحت، يمكن التنصت عليها خصوصاً إذا كان الاتصال يتم باستخدام البروتوكولات غير الآمنة مثل HTTPوFTP
- كما أنها ملعب البرمجيات الضارة بأشكالها المختلفة ومرتع للصيد بهدف الحصول على كلمات السر.

مستويات حماية المعلومات

❑ الربط مع الشبكة الخارجية LAN to WAN:

- يعبر عن النقطة التي يتم فيها اتصال الشبكة الداخلية مع الشبكة الخارجية (عادةً الإنترنت) ويتم من خلال أجهزة التحويل Routers، وهنا يجب أخذ احتياطات لها علاقة بمستوى وصول المستخدمين المحليين للشبكة الخارجية ومقدار وصول الشبكة الخارجية للشبكة الداخلية بضبط إعدادات الجدار الناري بشكل سليم، ممكن على سبيل المثال منع عمل بروتوكولات VPN وبالتالي لا يمكن استخدام برامج كسر بروكسي مثل Psiphone
- يمكن منع هذه البروتوكولات عن كل التجهيزات ماعدا أجهزة معينة بحيث يتم السماح لمسؤول الـ IT بالاتصال بالمواقع المحجوبة لتحميل البرمجيات المطلوبة، كما يجب تحديد المنافذ Ports التي يمكن للشبكة الخارجية الوصول إليها، مثلاً السماح بالاتصال على المنفذ 80 والمنفذ 443 للوصول إلى موقع المنظمة الداخلي بهدف السماح للموظفين بأداء أعمالهم من المنزل.
- بشكل عام يعتمد العمل هنا على ضبط إعدادات الاتصال مع الشبكة الخارجية وبناء سياسة محددة وصارمة تحدد الصلاحيات حسب المناصب والأعمال المتوجب على الموظفين القيام بها.
- لا يجب أن ننسى الحماية من هجمات DoS و.DDoS
- كما ينتشر في العمل ما يعرف باسم Cyberslacking وفيه يتكاسل الموظفون عن أداء مهاهم وذلك بتصفح مواقع الأنترنت مثل Facebook وYoutube وبالتالي يجب على العمل تحديد إمكانية وصول الموظفين إلى هذه المواقع.

مستويات حماية المعلومات

❑ الوصول عن بعد:

- تتم هذه الهجمات من خلال محاولة الوصول إلى الشبكة الداخلية من الخارج، ويمكن أن تتضمن محاولة كسر كلمات السر باستخدام هجوم القوة المفرطة Brute Force أو الهجمات القائمة على القواميس Dictionary Basedولحل هذه المشاكل يجب القيام بوضع سياسة لكلمات السر تجبر الموظفين على استخدام كلمات سر صعبة التخمين وتغييرها مرة 30أو 60 يوماً
- يجب أن نراعي إمكانية تسرب المعلومات الداخلية الخاصة بشكل أو بآخر عن طريق ثغرات في البرامج المستخدمة أو نتيجة خطأ من موظف أو ثغرة في إعدادات الحماية تترك النظام مفتوحاً للهجمات عن بعد
- يجب أن نقوم بتشفير البيانات المخزنة لضمان عدم إمكانية استثمارها من قبل القراصنة، كما يفضل اعتماد تشفير الأقراص في أجهزة الشركة المتنقلة التي تسلم إلى الموظفين) حاسب محمول مثلاً (وذلك في حال إضاعته لهذا الجهاز لا يمكن معرفة المعلومات المخزنة فيه.

مستويات حماية المعلومات

المخدمات والبنية التحتية:

- تتعلق بمستوى القوة والحماية الموجود ضمن المخدمات التي يتم التواصل معها وقدرتها على مقاومة الهجمات البرمجية المختلفة
- كما تتعلق بمقدار أمن البنية التحتية التي يتم من خلالها التواصل مع هذه المخدمات (أي لا أحد يتسمع على مكالماتك الهاتفية)
- بالإضافة لتواجد مخدمات إحتياطية في أماكن مختلفة للحماية من الكوارث البيئية.

